IN THE UNITED STATES DISTRICT COURT FOR THE

EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA

v.

SEAN MICHAEL MCLAUGHLIN,

Defendant.

UNDER SEAL

Case No. 1:19-mj-442

AFFIDAVIT IN SUPPORT OF A CRIMINAL COMPLAINT AND ARREST WARRANT

I, Raymond Abruzzese, being duly sworn, depose and state:

1. I am a Special Agent with the U.S. Department of Homeland Security ("DHS"), Homeland Security Investigations ("HSI"), and have been by employed by HSI since 2003. I am currently assigned to the Office of HSI, Washington, D.C. ("HSI DC"), and have investigated crimes relating to child exploitation on the internet since approximately October 2016.

2. I have advanced and on-the-job training in child exploitation on the internet and have participated in federal, multi-jurisdictional, and international investigations, many of which involved child exploitation and/or child pornography offenses. As part of my current duties as an HSI agent, I investigate criminal violations relating to child exploitation and child pornography, including violations pertaining to the illegal distribution, receipt, transportation, possession, and access with intent to view child pornography, in violation of 18 U.S.C. §§ 2252(a) and 2252A(a). I have received training in the area of child pornography and child exploitation and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256).

3. This affidavit is submitted in support of a criminal complaint and arrest warrant for Sean Michael McLaughlin ("MCLAUGHLIN") for a violation of Title 18, United States Code, Section 2252(a)(2), which makes it a crime to knowingly receive child pornography.

3. I am familiar with the information contained in this affidavit based upon the investigation that I have conducted, along with my conversations with other law enforcement officers, computer forensic agents and others, and my review of reports and database records.

4. This affidavit is submitted for the limited purpose of obtaining a criminal complaint and arrest warrant. It does not include each and every fact known to me or the government about the investigation. I have set forth only those facts that I believe are necessary to establish probable cause.

BACKGROUND FOR PEER-TO-PEER FILE SHARING, EMULE, SHAREAZA AND THE EDONKEY NETWORK

5. Peer-to-peer ("P2P") file sharing is a method of communication available to Internet users through the use of software downloaded from the internet. It is used to share digital files between different users of a P2P network. The hallmark of P2P file sharing is that users of a particular P2P network upload and download files to and from one another's computers, as opposed to a centralized server. As a result, the availability of a particular file on a P2P network at any given time depends on whether any other users are connected to the network and making that file available.

6. The eDonkey2000 ("eDonkey") network is one of several P2P file-sharing networks on the internet. It can be accessed by computers running many different client programs. These programs share common protocols for network access and file sharing. The user interface, features and configuration may vary between clients and versions of the same client.

7. Examples P2P clients, or file sharing applications, on the eDonkey network include eMule and Shareaza. Both eMule and Shareaza are open-source software programs available for free on the internet. The eMule and Shareaza software allow users to conduct keyword searches for files that are shared on the eDonkey network. When a keyword search is started, the search is sent out over a worldwide network of computers using compatible P2P software. The results of the keyword search are displayed to the user. The user then selects a file or files to be downloaded from the displayed results. When a user first sets up the P2P client, a folder on the computer is designated to store downloaded files. A file that is downloaded by the user is stored that designated area until moved or deleted by the user.

8. The eDonkey network's file-sharing capability is based on the eDonkey hash algorithm. This mathematical algorithm allows for the unique identification of files. The eDonkey hash algorithm is calculated by first dividing each file into 9,728,000 byte parts. The Message-Digest 4 (MD4) hash algorithm is then applied to each file part, starting with Part 0. The MD4 hash algorithm is then applied to the sequential concatenation of the MD4 hashes applied to each file part, thereby creating the unique eD2k hash value. If the file size is less than 9,728,000 bytes, then the eD2k hash of the file is equivalent to the MD4 hash. The MD4 hash is a 128-bit algorithm typically represented as 32-digit hexadecimal numbers. The eDonkey Hash is called "secure" because it is computationally infeasible for two files with different content to have the same eDonkey hash value.

10. Based on my training, experience, and discussions with other trained law enforcement officers, I know the following facts about the eDonkey network and eMule and Shareaza software:

a. The eDonkey network is frequently used in the online trading of child pornography. It is used to trade digital files including still images and movie files of child pornography.

b. During the installation of eMule and Shareaza, which requires the user to provide a "shared" folder, various settings are established that configure the host computer to share—*i.e.*, distribute—files. For each file located in a user's shared directory, eMule and Shareaza processes the file and computes an eDonkey hash value.

c. Users of the eDonkey network may receive a selected file from numerous sources by accepting segments of the file from multiple users and then reassembling the complete file on the local computer. The network uses eDonkey hash values to ensure that exact copies of the same file are used during this process.

d. When a user connects to the eDonkey network, a list of shared files, descriptive information, and their associated eDonkey hash values are made searchable to allow other computers on the eDonkey network to search for and locate these files.

11. Law enforcement has modified the standard eMule software to only allow the downloading of a single file from a single IP address, as well as the displaying of additional information about the source file and the source user.

12. Law enforcement agencies have compiled databases of known files containing child pornography or child erotica that are checked against files being distributed over P2P networks. For the eMule programs used by law enforcement, this list is known as a "Files of Interest" list.

The "Files of Interest" list contains files that have been previously viewed by law enforcement officers and determined to contain suspected child pornography or child erotica. The eMule program used by law enforcement also tracks Files of Interest associated with the Shareaza P2P application.

PROBABLE CAUSE

A. Background on the Investigation

13. In or about August 2017, I began investigating an individual who was using the Internet Protocol (IP) Address 173.73.189.161 (the "Target IP") to access the Internet. This investigation pertained to the use of the Shareaza P2P software that had been used to receive and distribute digital child exploitation material. I

14. In August 2017, I was able to make a direct connection with the Target IP. During this direct connection, I downloaded the following video files from the Target IP:

a. *File name*: [boy+man] man fuck boy-Hotondad - Rare !.avi

eDonkey hash value: 1EBE38EC2E0DE550F0EB316C02B9AEC3

Video description: The video is approximately 30 seconds in length. This file depicts a nude, prepubescent male. The prepubescent male does not have any visible pubic hair, chest hair, or underarm hair. The prepubescent male also has young-looking facial features. An adult male sitting on a blue couch is anally penetrating the prepubescent male. The adult male is also seen touching the prepubescent male's penis.

b. *File name:* [man and boys #1] ru-mb#1_04 - Man fucks 14yo russian boy.mpg

eDonkey hash value: EA7B8AD2EC6FD07D2F68D748A575B147

Video description: The video is approximately 11:13 minutes in length. The video begins with a minor male lying in a bed with no shirt and his jeans pulled down exposing his genitalia. The minor male has a small amount of pubic hair but does not have any chest or underarm hair visible. An adult male lies next to the minor and begins to penetrate the minor anally. During the video, the adult male moves the minor into different positions. The minor male's facial expression appears to indicate that he is in pain or some level of discomfort during the video.

c. *File name:* p-101 boyorgie pthc pedo kdv 8yo 9yo 10yo 5 little gay boys young boylovers fuck suck.mpg

eDonkey hash value: 8CA216BE0BCC8A5FB74A5634907CFE56

Video description: The video depicts several naked, prepubescent males. All of the prepubescent males depicted in this video conduct sexual acts on each other. In a portion of this video one of the prepubescent males has his hands tied up with a rope while another prepubescent boy penetrates his anus. Another scene in this video depicts a prepubescent male with his hands and feet tied up with rope while another boy inserts his penis into that prepubescent male's mouth.

d. *File name:* [boy+man] jason4.AVI

eDonkey hash value: 94A3537552AE28450C06059958C09780

Video description: This video is approximately 6:52 minutes in length. In this video a prepubescent male is depicted naked kneeling on a bed. The minor male has no pubic hair, chest hair, or underarm hair. The camera zooms in on the prepubescent males' anus and penis. The prepubescent male is shown placing his finger in his anus. Later in the video an adult male is shown touching the minor male's penis. The minor male then has tape placed over his mouth and is handcuffed. The adult male penetrates the prepubescent male's anus.

15. I obtained information from Verizon Fios via legal process. According to Verizon Fios, during the time that I downloaded the child exploitation material as referenced above from the Target IP, the Target IP was assigned to a residential address located in Falls Church, Virginia. MCLAUGHLIN's mother was the listed subscriber.

16. In and about October 2017, I conducted record checks via a law enforcement database, which indicated that an individual named Sean McLaughlin was issued a Virginia driver's license and that the address listed on this driver's license was the address located in Falls Church, Virginia. Further this database indicated that a red Jeep was registered to MCLAUGHLIN and his mother at this same address. In or about December 2017, I conducted additional record checks via the same law enforcement database. At that time, the address listed on

MCLAUGHLIN's driver's license and the registered address for the above described red Jeep was changed to an apartment located in Alexandria, Virginia.

17. In or about January 2018, I received information about this apartment located in Alexandria from Cox Communications via legal process. According to Cox Communications, there was an account listed for an individual and the IP Address assigned to this subscriber by Cox Communications during the time period of September 14, 2017 through January 5, 2018 was 70.174.164.86.

18. In or about January 2018, I conducted a database check via a law enforcement database that collects the IP addresses of some computers making suspected child sexual abuse material available for download on P2P networks. According to this database the IP Address 70.174.164.86 was associated with downloading more than ten files of suspected child exploitation material during the time period of September 14, 2017 through January 5, 2018.

B. **Interview with Sean McLaughlin**

19. On or about January 25, 2018, I traveled to the apartment in Alexandria. I knocked on the front door to the apartment a few times; however, nobody answered. I left a business card and requested that MCLAUGHLIN call me. On or about January 25, 2018, at approximately 1:00 p.m., I received a phone call from MCLAUGHLIN. MCLAUGHLIN agreed to meet with and talk with me later that afternoon. MCLAUGHLIN stated I could come to his residence at 6:00 p.m.

20. On January 25, 2018 at approximately 6:00 p.m., I and another agent traveled to MCLAUGHLIN's apartment. I identified myself as law enforcement and requested permission to enter MCLAUGHLIN's apartment. MCLAUGHLIN invited myself and the other agent inside and stated we could sit down on a couch located near the front door. MCLAUGHLIN stated he had moved into this apartment in September 2017 and that prior to moving into this apartment he

lived with his mother at the residence located in Falls Church. MCLAUGHLIN stated, prior to moving out of his mother's residence, it was only he and his mother that were living at the Falls Church residence. MCLAUGHLIN stated he was familiar with P2P file sharing programs and that he has used eMule and Shareaza. MCLAUGHLIN stated he had downloaded material from these programs to include pornography. MCLAUGHLIN estimated his last downloads from eMule or Shareaza were in September 2017. MCLAUGHLIN stated he uses his laptop to view the downloaded material.

21. I explained to MCLAUGHLIN that I knew someone was downloading files that depicted child sexual exploitation material at this previous address in Falls Church, and that it appeared someone was downloading child sexual exploitation material at his current residence. MCLAUGHLIN stated he has periods when he downloads material that depicts child sexual exploitation material. MCLAUGHLIN stated he downloads this material because he finds it sexually stimulating and that he masturbates to the material. MCLAUGHLIN stated he has used a computer tablet and a laptop to obtain and view files that depict child sexual exploitation material. MCLAUGHLIN stated he was not one hundred percent sure how the file sharing program worked but knew he could search for material and download it. MCLAUGHLIN stated that after he downloads the material he deletes the files and then uninstalls the program. MCLAUGHLIN estimated that he had downloaded fifty videos that contained child sexual exploitation material in the past year. MCLAUGHLIN again stated he found this material from typing in key words into the P2P program(s).

22. MCLAUGHLIN stated he was a registered nurse and that he worked in the emergency room at the Virginia Hospital Center.

23. MCLAUGHLIN provided his verbal and written consent for HSI to conduct a complete search of his Red Asus Tablet (SN: E7N0BC136239307) and his Red Dell Alienware Laptop (SN: JBFNDS1). MCLAUGHLIN provided passwords/codes to access the listed computer tablet and laptop. I detained and transported these items to an HSI office located in Sterling, Virginia, where they were placed into a secure HSI facility.

C. **<u>Computer Forensic Analysis of ASUS Tablet</u>**

24. A forensic analysis of the previously identified Red Asus computer tablet, revealed that the registered owner of this device is seanmmcl@verizon.net. The user name on the tablet is listed as seanm_000 and the given name Sean McLaughlin. The user name seanm_000 is the only account listed as active on this device and it is password protected. The forensic analysis further revealed this device contained approximately 13 videos depicting child pornography and 118 image files depicting child pornography. These video and image files include what appear to be prepubescent children engaged in sexual activity with themselves, other children, and adults. The images involved mostly minor males ranging from infant through early teenage years, and some of the images involved bondage. The following is an example of a file that depicts child pornography that was located on the red Asus tablet:

a. *File name*: (pedo boy) Toddler Rape.avi_000037400_2.jpg

   File path: Users\Seanm_000\AppData\Roaming\Shareaza\Collections\Men fuck preteen boys with picture preview.Collection

   Image description: This image depicts an infant to toddler-aged male lying on his stomach with a pillow over the back of his head. The infant male's diaper is removed and a hand belonging to an adult can be seen using a finger to penetrate the infant male's anus.

b. *File name*: Pedo (Yamad Boy)Older White Man Fucks A Cute Skinny Thai Teen Twice (Hot!!!).mpg_001383293_2.jpg.

File path: Users\Seanm_000\AppData\Roaming\Shareaza\Collections\Men fuck preteen boys with picture preview.Collection.

Image description: This image depicts an adult naked male who appears to be penetrating a minor male's anus with his penis.

c. *File name*: Gay Pedo - preteen-Zach1-man fucks 7yo boy.mpg_000173037_2.jpg.

File path: Users\Seanm_000\AppData\Roaming\Shareaza\Collections\Men fuck preteen boys with picture preview.Collection.

Image description: This image depicts a prepubescent male's anus being penetrated by an adult male's penis.

25. The P2P Software program "Shareaza" had been installed on October 7, 2017 on the Asus tablet and was located in the root\Program files\Shareaza. The Shareaza Library file contained a list of the user's recently downloaded files. The Shareaza library was found with in the file location: C:\users\seanm_ooo\appdata\roaming\shareaza\torrents. A review of the file's names that are contained within the Shareaza Library file folder includes files that have names that I know through my training and experience are indicative of or likely to depict child pornography to include: "(pthc) niño se come un pene enorme(2).mpg.torrent" and "11yo Preteen BJ + Anal Fuck With 10yo Boy Neighbor and His Dad.AVI.torrent."

26. Shareaza keyword search contains search queries performed by the user. Some of the queries include terms that I know through my training and experience are indicative of or likely to contain child sexual abuse material. Examples of the Shareaza search terms are: "15yo boy fuck -girl -sister -woman -mom," "boy 9yo -woman -sister -mom -girl," and "boy fuck 7yo -woman -sister -mom -girl."

27. LNK files are created automatically by the computer for quick retrieval of files. LNK files are created after a user has opened a file. LNK files were located on the Asus tablet that I know are indicative or likely to contain child sexual abuse material. The LNK files referenced

in this paragraph were all found within the file path C:\users\seanm_000\downloads. Examples of LNK files that were found on the Asus tablet are: "Zz-097- Man Fuck 12Yo Boy.avi;" "PTHC - Boyfuck – German - 6yo and 11yo Boys Fucked in a Car - Priv001b_11J - 34m40s_Trimmed2.mp4;" "7yo Piss On Dad Pthc Pedoland Frifam New Pasi Opipi, Boy and Dad.mpg;" "[boy+man] jason4.AVI." The final example was accessed by the user of this computer on June 14, 2016. This file also matches the name of a file associated with the use of Shareaza as described in paragraph 14 of this affidavit.

28. Microsoft Internet Explorer is a program included with the Microsoft Windows operating system used to access web sites on the internet and access files stored locally on the computer. Internet Explorer activity observed during the forensic review of the Asus Tablet revealed that within the folder "OS\Users\SeanM_000\AppData\Local\Microsoft\Windows\webcache" is the file named, WebCacheV01.dat. A review of Internet Explorer activity shows access to files that contain names, which I know in my training and experience are indicative of or likely to contain child pornography. Examples of the file names contained within the WebCacheV01.dat file that were viewed from the file path C:Users\seanm_000\downloads are listed below:

a. Accessed on November 2, 2017: "yoBoys-Man-10yo-Small-Hole-and-13yo-Boys-Deeply-Anal-Fucked-By-Man-Big-Cock-Privado04-RealSound-36m36s.mpg;"

b. Accessed on October 16, 2017: "((((BoyLove)))) Dad & Boy 12yo.avi;" and

c. Accessed on October 16, 2017: "Pthc – Boyfuck - p101 - mikael 10Yo - 07m10S.mpg."

The Internet Explorer Activity shows access to hundreds of images and videos files containing child pornography from 2002 through 2018. This activity includes entries on August 16, 2017 where the Windows user "seanm_000" is accessing links associated with nursing school or training and viewing child pornography videos on the same day.

29. Jump Lists also known as AutomaticDestinations and CustomDestinations, are a feature of the windows operating system to provide the Windows user quick access to recently opened files for specific applications in the Windows Task Bar. AutomaticDestinations are created by the operating system when the user performs an action such as opening a file or playing a video. CustomDestinations are created when the user manually pins a file to the application in the TaskBar. The operating system creates a separate Jump List file for each program used by the computer user. The folder "Root\Users\Seanm_000\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations" contains information about images and videos accessed by the computer user. A list of videos viewed by the computer user include numerous file names that I know from my training and experience are indicative of or likely to contain child pornography. Some examples of these video titles are: "!!! Mb1 Pjk Rape (27Min) s00-Zz-087- Man Fuck 10 11Yo Boys Part 1 Dad And Horny Pervert! 10Yo Son Abuse 11O Boy In The Forest.avi;" (Boy) 10Yo Boy Fucked By Dady And Step-Brother.avi;" and "p-101 boyorgie pthc pedo kdv 8yo 9yo 10yo 5 little gay boys young boylovers fuck suck.mpg." The final example was accessed by the user of this computer on May 27, 2017. This file also matches the name of a file associated with the use of Shareaza as described in paragraph 14 of this affidavit.

30. In addition to the information set forth above, documents and files located on the Asus Tablet also directly associate the user of the Tablet with MCLAUGHLIN. Some of these files and documents were located in the downloads folder associated with the Seanm_000 user account including:

a. Self evaluation Sean.docx, a document with the name "Sean Michael McLaughlin" in the top corner that appears to be a work-related performance assessment.

b. McLaughlin_Sean_Resmue.docx, which appears to be a resume for MCLAUGHLIN showing that he was working as a nurse extern at the time.

c. McLaughlin_Sean_Coverletter.docx, which is a letter dated February 28, 2017, from "Sean Michael McLaughlin" seeking employment as a nurse with the Inova Alexandria Emergency Department.

31. Further named files located on the Tablet as Jump Lists directly associate the use of the Tablet with MCLAUGHLIN. Some of these file names include: "Pediatric Nursing_Respiratory.ppt;" "Sean McLaughlin Treatment for Lead Poisioning.docx;" and "NURS 453 Research\McLaughlin.docx."

D. **Computer Forensic Analysis Dell Alienware Laptop**

32. A forensic analysis of the previously identified Dell Alienware Laptop revealed that this device contained no less than 40 videos, which depict child pornography, to include what appear to be prepubescent children engaged in sexual activity with themselves, other children, and adults. The following is an example of one of the video files that in my training and experience depict child pornography and that was located on the Dell Alienware Laptop. This file was located within the file path:\ Users\Sean\AppData\Local\Shareaza\Incomplete: Preview of + [MB] Jason Boy 3 And Man Sex (full)_2.mpg. The file depicts a prepubescent male who exposes his genitalia. The camera zooms in on the prepubescent male's genitalia. Further the prepubescent male uses his hand to masturbate. Additionally, an adult male uses his fingers to masturbate the prepubescent male.

CONCLUSION

33. The fact that a portion of the video files described in this affidavit were located within a folder using the name "download" or a variance of the name download would indicate that the video files were obtained from the internet. Further the documented use of Shareaza to obtain image and video files demonstrate that the tablet user was obtaining child pornography from the internet. The fact the tablet user is typing internet search terms that are indicative of child pornography and that the titles of the images and videos located on the highlighted devices have terms such as "Pthc" and "10 yo, 11yo" demonstrate that the user was actively and intentionally searching for child pornography. Lastly, when interviewed McLaughlin stated he was using Shareaza to obtain child pornography.

34. For the foregoing reasons, I submit to the Court that there probable cause to believe that Sean MCLAUGHLIN has knowingly received child pornography, in violation of 18 U.S.C. § 2252(a)(2). I, therefore, respectfully request the attached arrest warrant be issued authorizing the arrest of MCLAUGHLIN.

Respectfully submitted,

Raymond Abruzzese
Special Agent
Homeland Security Investigations

Subscribed to and sworn before me on October 10th 2019.

/s/
Michael S. Nachmanoff
United States Magistrate Judge

The Honorable Michael S. Nachmanoff
United States Magistrate Judge
Alexandria, Virginia